

-2-

REMARKS

The Examiner has rejected Claims 1, 12, and 23-27 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner has stated that in the following claim limitations, it is unclear what is configured, the module or the execution of the modules:

“wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;”

“wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.”

Applicant respectfully asserts that the above claim limitations clearly state that “the commands execute the risk-assessment modules in a specific manner that is configured,” and thus it is the manner of execution of the modules that is configured.

The Examiner has further rejected Claims 1, 4-6, 9-10, 12, 15-17, 20-21, and 23-35 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No.: 6,298,445) in view of Orchier et al. (U.S. Patent No. 6,070,244). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 12, 23 and 24, the Examiner has relied on the following excerpt from Shostack to meet applicant’s claimed “wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer.”

“The network scan for IP devices is invoked using the properties (PROP) icon 72 which enables an authorized local user 6 to configure the various modules.” (Col. 12, lines 55-57) (emphasis added)

Applicant respectfully asserts that the above excerpt from Shostack clearly *teaches away* from applicant’s claim language by disclosing a properties icon that “enables an authorized local user to configure the various modules.” Applicant, on the other hand, claims that the

-3-

"commands execute the risk-assessment modules in a specific manner that is configured at the remote computer."

Furthermore, the Examiner has relied on the following excerpt from Orchier to make a prior art showing of applicant's claimed, "wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters."

"The manual maintenance agent 86 takes inputs from the user and converts them into platform independent security maintenance instructions which are then processed by the maintenance agent abstraction facility 90. Examples of platform independent security maintenance categories and data are as follows:
AddUserAccount(id, platformList, name, Payroll Number, expenseCode)
RemoveUserAccount(id, platformList)
AddUserAccountToGroup(id, platformList, GroupName)
RemoveUserAccountFromGroup(id, platformList, GroupName)
ModifyUserAccountName(id, platformList, name)
ModifyUserAccountPay(id, platformList, Pay)
ModifyUserAccountExpenseCode(id, platformList, expenseCode)
DisableUserAccount(id, platformList)

FIG. 8c shows the screen used to designate how often data should be collected. FIG. 8d shows the screen used to designate the server from which data should be collected. FIG. 8e shows the screen used to designate high risk applications. FIG. 8f shows the screen used to designate the environment. FIG. 8g shows the screen used to designate high risk reports. FIG. 8h shows the screen used to designate event code mapping of native codes to the common system code." (Col. 14, lines 25-52)

Applicant respectfully asserts that the above excerpt from Orchier suggests taking inputs from a user regarding user accounts (see exemplary categories and data in above excerpt) and then converting those inputs into instructions to be processed by a maintenance agent. Thus, Orchier's user inputs regarding user accounts simply fail to meet applicant's "commands [that] are processed by extracting parameters...and executing the risk-assessment modules...utilizing the associated parameters. To emphasize, simply nowhere in Orchier is there any suggestion of "extracting parameters" or utilizing such parameters in "executing the risk-assessment modules," as claimed by applicant.

-4-

With respect to independent Claims 25-27, applicant respectfully asserts that such claims are not met by the Shostack and Orchier references for substantially the same reasons as given above with respect to independent Claims 1, 12, 23 and 24.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

With respect to the dependent claims, applicant has carefully reviewed the excerpts relied upon by the Examiner to reject the same, and has found serious deficiencies in the Examiner's application of the prior art. Just by way of example, the Examiner relies on the following excerpt from Orchier to meet applicant's claimed "wherein the risk-assessment modules are selected for the agent based on specifications of the local computer" (see Claim 4 et al.).

"The security domains 70a-70n communicate with collection agents 72a, 72b, 72c . . . 72n, respectively. These collection agents 72a-72n, a part of security administration system 50, represent software facilities written specifically for the corresponding operating system or system software components, for example the workstation server, LAN or NetWare.TM. software facility comprising the security domains 70a-70n. Therefore, there are many different collection agents, each of which is associated with a specific security domain type. The present invention has been reduced to practice with collection agents specific to NetWare.TM. 3.1, NetWare.TM. 4.0, Windows NT, two different remote access servers, RACF, ACF2, Sybase, Oracle, AS 400, VAX/VMS, Tandem, Lotus Notes, four different UNIX operating systems and an Internet

-5-

firewall.

The collection agents 72a-72n use system utilities and/or APIs (Application Programming Interfaces) to extract from the individual security domains 70a-70n specific data defining security information pertaining to the system users, passwords, security groups, and where applicable: permissions, access controllers, logon events, file access events, system management events, file attributes, software and hardware versions, password control parameters, system parameters and the like. The information they collect is passed to the collection agent abstraction layer or facility 74 for further processing." (Col. 4, line 48-Col. 5, line 6 - emphasis added)

After carefully reviewing such excerpt and the remaining Orchier reference, however, it is clear that Orchier merely suggests security domains with collection agents each written for a specific domain type. Applicant notes, however, that Orchier also states that the collected data is analyzed to determine if user and system data comply with security policy requirements (Col. 7, lines 37-39). Thus, a specific collection agent is chosen according to the type of data to be collected. Choosing a collection agent for collecting data in order to further determine whether user and system data comply with security policy requirements, as taught in Orchier, simply fails to meet selecting "risk-assessment modules...based on specifications of the local compute," as claimed by applicant.

Still yet, the Examiner relies on col. 12, lines 27-40; col. 12, lines 58-67; col. 12, lines 41-57; col. 12, lines 23-34; and col. 12, lines 14-20 from Shostack to meet applicant's claimed "wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a REaddir module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGrent module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command" (see Claim 5 et al.).

Applicant respectfully disagrees with this assertion. Shostack completely fails to even suggest "a STAT module for performing a stat system call on a file, a READ module for reading a file, a REaddir module for returning contents of a directory, a FIND module for locating a list of files based on a given function...[and] a GETGrent module for retrieving an entry from a group database."

-6-

The above cited references in Shostack merely disclose that “[t]he first module uses...[a] checksum” (col. 12, lines 27-29), “the second module performs a network scan...the network scan produces a map of the network” (col. 12, lines 44-48), “the third module...compare[s] and identif[ies] vulnerable passwords” (Col. 12, lines 61-63). Thus, it is clear that there is no mention or suggestion in Shostack of a STAT, READ, READDIR, FIND, and/or GETGREN module, as required by applicant’s claims.

With respect to dependent Claim 31, the Examiner has relied on the following excerpt from Shostack to make prior art showing of applicant’s claimed “wherein the feedback includes descriptions as to how to correct the vulnerabilities.

“The present invention provides such a mechanism by automatically providing enhancements to a database of security vulnerabilities and using that information to provide security solutions to potentially “weak” computer networks and/or computers.” (Col. 4, lines 8-12 - emphasis added)

“The GUI 70 may also provide a reporting mechanism. The GUI 70 may also include several means for reporting various network transactions. In the disclosed invention, the GUI 70 includes a log view 80 may allow a user to view a text version the update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log.” (col. 13, lines 36-44)

Applicant respectfully disagrees. In the above cited excerpts as relied on by the Examiner, Shostack teaches automatically providing enhancements and providing security solutions to vulnerable computers. The only reporting Shostack discloses relates to logs of an update process, storage device, and security vulnerabilities. Thus, Shostack suggests automatically providing enhancements and solutions to security vulnerabilities without ever giving descriptions on how to correct the vulnerabilities. For these reasons, the Shostack reference clearly fails to meet applicant’s claimed “wherein the feedback includes descriptions as to how to correct the vulnerabilities.”

With respect to dependent Claim 35, the Examiner has rejected such claim limitations based on col. 4, lines 48-62 of Orchier. Applicant respectfully asserts that the Orchier reference fails to meet applicant’s claimed “wherein a different set of risk-assessment modules exist on

-7-

different local computers, based on a platform associated with each of the local computers" for reasons substantially similar to those given with respect to dependent Claim 4 above.

The Examiner has also rejected Claim 11 et al. under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. and Orchier et al. in further view of Smid et al. (U.S. Patent No. 4,386,233). Applicant respectfully disagrees with such rejection.

Specifically, the Examiner has relied on the following excerpt from Smid to make a prior art showing of applicant's claimed "wherein commands are decrypted utilizing a shared key."

"Alternatively, authentication is accomplished by controlling access to the cryptographic function by encrypting user commands with a cryptographic function using a password supplied by the user as the cryptographic key and then **decrypting the encrypted commands using a prestored version of the password as the cryptographic key.**" (Col. 3, lines 5-12 - emphasis added)

Applicant respectfully asserts that Smid teaches "decrypting the encrypted commands using a prestored version of the password," which fails to meet the specificity of applicant's utilization of a "shared key." It is noted that a prestored version of a password as a key does not meet applicant's claimed "shared key" since a prestored version of a password does not have any bearing on whether the key is shared.

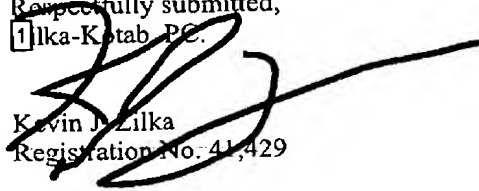
Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

-8-

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NA11P011/01.116.01).

Respectfully submitted,
[i]lka-Kotab, PC.


Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100